(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－332019
（P2001－332019A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数４　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－144456(P2000－144456)

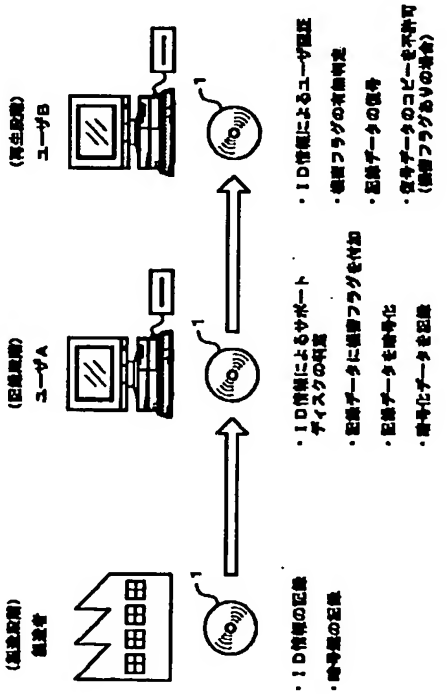
(22)出願日　平成12年５月17日(2000.5.17)

(71)出願人　000204284
太陽誘電株式会社
東京都台東区上野６丁目16番20号
(72)発明者　大村　幸秀
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(72)発明者　砂川　隆一
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(74)代理人　100096699
弁理士　鹿嶋　英實

最終頁に続く

(54)【発明の名称】　ライトワンス型光ディスク用データ記録再生方法、ライトワンス型光ディスク用データ再生装置および記録媒体

(57)【要約】
【課題】　再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスク用データ記録再生技術を提供する。
【解決手段】　ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込み、前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する。再生データの再利用を阻止し、再生段階におけるセキュリティを確保できる。



1

【特許請求の範囲】

【請求項1】　ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込む書き込み工程と、

前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する複製制限工程と、

を含むことを特徴とするライトワンス型光ディスク用データ記録再生方法。

【請求項2】　前記光ディスクのシステム領域に格納されたセキュリティ情報に基づき該光ディスクへのアクセスを制限するアクセス制限工程をさらに具備することを特徴とする請求項1記載のライトワンス型光ディスク用データ記録再生方法。

【請求項3】　ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を備えたことを特徴とするライトワンス型光ディスク用データ再生装置。

【請求項4】　ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を実現するためのプログラムを格納したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ライトワンス型光ディスク用データ記録再生方法、データ再生装置および記録媒体に関する。詳しくは、1回だけデータを書き込むことができるCD-R（Compact Disc Recordable）に代表されるライトワンス型光ディスクに適用するデータ記録再生方法、データ再生装置および記録媒体に関する。

【0002】

【従来の技術】各種コンテンツやコンピュータプログラム等の電子データの配布媒体に、CD-ROM（Compact Disc Read Only Memory）が多用されている。CD-ROMは、電子データを記録したマスタCDからプレス成型等によって製造される複製物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版CDやプライベートCDなどには、データの消去や上書きができない（追記は可能）ライトワンス型の光ディスク装置、典型的にはCD-Rが用いられる。

2

CD-Rは透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点でCD-ROMと構造上の違いがあり、専用の記録装置（CD-Rライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ピットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【0003】CD-Rは、上記のとおりデータの消去や上書きができないライトワンス型の記録媒体である。すなわち、一度書き込んだデータの消去や書き換えが不可能である。そのため、不正者によるデータの消去や改ざんを確実に防止できるという優れた利点を持つことから、今日、特に秘匿を要する電子データの保管や配布などの用途に欠かせない記録媒体としての地位を確立しているが、反面、CD-Rは記録情報の読み出しが自由であるが故に、情報の不正読み出しや不正コピーを防止できないという欠点も持っている。

【0004】そこで、秘匿を要するデータを記録する際に、例えば、図16に示すように、暗号化して記録することが行われている。図において、平文データ100は暗号化前の“生”のデータであり、例えば、可読性を有するテキスト形式のデータである。この平文データ100を不可視化して記録する場合、まず、所定の暗号化ツール101を用いて暗号化データ102に変換する。暗号化の方式は特に限定しないが、暗号鍵と復号鍵に共通の鍵を用いる共通鍵方式である。以下、この鍵のことを代表して「暗号鍵」ということにする。したがって、以下において、暗号鍵という場合は復号鍵も意味することとする。

【0005】さて、暗号化されたデータ（図においては暗号化データ102）は不可視データであり、そのまま配布しても安全（計算量的に安全）であるため、この暗号化データ102をCD-R103に書き込むことによってデータの不正読み取りを防止し、セキュリティを保つことができる。再生の際は、CD-R1から暗号化データ104を読み出し、所定の復号ツール105を用いて平文データ106に戻せば（復号すれば）よい。

【0006】

【発明が解決しようとする課題】しかしながら、上記のセキュリティ対策にあっては、復号後のデータ（平文データ106）の再利用が自由であり、データ保全の効果はもっぱらCD-R103に収められた状態でしか得られないという不都合がある。すなわち、CD-R103から読み出されて復号された後の平文データ106については、まったくセキュリティがかかっておらず、この平文データ106に対するデータ保全は単に再生側ユーザのモラルに期待するしかないという問題点があった。

【0007】したがって、本発明が解決しようとする課題は、再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以って、記録か

ら再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスク用データ記録再生技術を提供することにある。

【0008】

【課題を解決するための手段】請求項1記載のライトワンス型光ディスク用データ記録再生方法は、ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込む書き込み工程と、前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する複製制限工程と、を含むことを特徴とする。これによれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が制限される。請求項2記載のライトワンス型光ディスク用データ記録再生方法は、請求項1記載のライトワンス型光ディスク用データ記録再生方法において、前記光ディスクのシステム領域に格納されたセキュリティ情報に基づき該光ディスクへのアクセスを制限するアクセス制限工程をさらに具備することを特徴とする。これによれば、光ディスクのシステム領域に不可視状態で格納されたセキュリティ情報に基づいて光ディスクへのアクセスが制限される。請求項3記載のライトワンス型光ディスク用データ再生装置は、ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、を備えたことを特徴とする。これによれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が禁止される。請求項4記載の記録媒体は、ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、を実現するためのプログラムを格納したことを特徴とする。これによれば、マイクロコンピュータを含むハードウェアリソースと該プログラムとの有機的結合によって前記判定手段および禁止手段が実現される。

【0009】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、以下の説明における様々な細部の特定ないし実例および数値や文字列その他の記号の例示は、本発明の思想を明瞭にするための、あくまでも参考であって、それらのすべてまたは一部によって本発明の思想が限定されないことは明らかである。また、周知の手法、周知の手順、周知のアーキテクチャおよび周知の回路構成等（以下「周知事項」）についてはその細部にわたる説明を避けるが、これも説明を簡潔にするためであって、これら周知事項のすべてまたは一部を意図的に排除するものではない。かかる周知事項は本発明の出願時点で当業者の知り得るところであるので、以下の説明に当然含まれている。

【0010】まず、本実施形態のライトワンス型光ディスク（以下「CD-R」という。）の利用形態を大まかに説明する。図1は、本実施形態のCD-R1の利用模式図である。この図では、製造者（メーカ）によるCD-R1の製造段階、ユーザAによる当該CD-R1への秘匿を要するデータの記録段階、および、ユーザBによる当該記録済みCD-R1からデータを読み出して再生する再生段階の三つの段階が示されている。

【0011】後の説明からも明らかになるが、（1）製造段階ではCD-R1に固有の識別情報（以下「ID情報」という。）と所定の暗号化方式における暗号鍵（復号鍵を兼ねるもの）とをCD-R1に電子的に記録して出荷する。ID情報と暗号鍵の記録場所はユーザからの直接的なアクセスが許可されていない場所（システム領域；領域構造については後述する。）である。（2）記録段階ではそのCD-R1のID情報から当該CD-R1が所定の製造者またはあらかじめ登録された製造者によって作られたもの（以下「サポートディスク」という。）であるか否かを判定し、サポートディスクである場合に、記録データに所定の“機密フラグ”を付加すると共に、CD-R1に書き込まれている暗号鍵を用いて記録データ（機密フラグを付加したもの）を暗号化し、その暗号化データをCD-R1に記録する。（3）再生段階ではCD-R1のID情報を用いてユーザ認証を行い、正規ユーザ（ID情報を知っているユーザ）に対してのみ暗号化データの復号処理を許容すると共に、復号データのコピーや保存等の複製処理を実行して再利用を行う場合は、記録データ中の“機密フラグ”の有無を判定し、機密フラグ有りの場合は上記再利用を拒否、例えば、コピー動作や保存動作を強制中断する。

【0012】これら三つの段階において、CD-R1にセキュリティを持たせるための工夫は、①製造時にCD-R1のシステム領域にID情報と暗号鍵を書き込むようにしたこと、②ユーザAによる記録時に、記録データに“機密フラグ”を付加するようにしたこと、③同記録時に記録データ（機密フラグ付）を暗号化してCD-R1に書き込むようにしたこと、④ユーザBによる再生時にID情報によるユーザ認証を行って正規ユーザに対してのみ暗号化データの復号を許可するようにしたこと、⑤同再生時に復号データの再利用が行われる場合は機密フラグの有無を判定して機密フラグ有りの場合にその再利用動作を強制中断するようにしたことにある。

【0013】①のID情報はデータ再生時のユーザ認証に用いられ、また、①の暗号鍵はデータの暗号化と正規ユーザによって行われる暗号化データの復号に用いられる。これらのID情報と暗号鍵はCD-R1の記録領域のうちユーザアクセスが許可されていない領域（システ

ム領域）に書き込まれた、いわば不可視化された“隠しデータ”である。①のＩＤ情報はまたデータ書き込み時におけるサポートディスクの判定にも用いられる。サポートディスクとは、前記のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたＣＤ－Ｒ１のことであり、正確には“機密フラグ”を用いて行われる復号後データの再利用禁止対策を“サポート”した特別なディスク（ＣＤ－Ｒ１）であることを意味する。

【００１４】ここで、機密フラグはその名前のとおりフラグ形式のデータであってもよいし、フラグ以外の別形式であってもよい。留意すべき点は機密フラグ（または機密フラグと同等のもの）の存在がユーザに対して秘匿化されていなければならないことにある。一般にフラグ形式のデータは二値論理（ブーリアン型ともいう。）の１ビットデータであり、そのビット位置を非公開とすることによって一応の秘匿化は可能であるが、総当りで調べられた場合にフラグの位置が見破られるおそれを否定できないため、望ましくは、電子透かしのような積極的な秘匿化対策を講じたデータとすることが好ましい。電子透かしとは、オリジナルデータの品質を損なうことなく、そのオリジナルデータの周波数、空間または時間の一つまたは複数のドメインに所定のメッセージ情報を隠す（埋め込む）ことをいう。機密フラグは、再生段階において、復号後の平文データの再利用（平文データを他の記録媒体にコピーや保存したりすること；複製動作ともいう。）を禁止するためのチェックフラグとして用いられる。これにより、暗号化データによるＣＤ－Ｒ１のセキュリティに加え、復号後の平文データのセキュリティ対策も講じることができ、本願発明の課題である、再生側ユーザのモラルに依存することなく復号後の平文データの再利用を禁止でき、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスクを提供することができるのである。

【００１５】以下、上記課題達成に必要な構成および作用について、具体例をあげて説明する。図２は、本実施形態におけるＣＤ－Ｒ１の外観図（ａ）およびその要部拡大図（ｂ）である。これらの図において、ＣＤ－Ｒ１は、直径１２ｃｍ（直径８ｃｍのものもある。以下、直径１２ｃｍのもので説明する。）のディスク状を有しており、ディスクの中心に直径１５ｍｍのセンターホール１ａが形成されている。ディスクの中心Ｔ０からセンタホール１ａの壁（ディスク内縁Ｔ１）までの距離は７．５ｍｍ、Ｔ０からディスク外縁Ｔ７までの距離は６０ｍｍであり、このＴ１～Ｔ７の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にＰＣＡ（Power Calibration Area）、ＰＭＡ（Program Memory Area）、リードイン（図では「ＲＩ」と略している。）、データエリア（図では「ＵＡ」と略している。）およびリードアウト（図では「ＲＯ」と略している。）の各領域が設けられている。

【００１６】各領域を概説すると、Ｔ２～Ｔ３に位置するＰＣＡは、ＣＤ－Ｒ１にデータを記録する際に行われるレーザ強度調整のための試し書き領域である。この試し書きは一般に１００回程度可能であり、少なくとも１回のデータ記録で１回分の領域を消費する。Ｔ３～Ｔ４に位置するＰＭＡは、ＣＤ－Ｒ１でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始／終了位置を一時的に保存する領域である。Ｔ４～Ｔ５に位置するリードイン（ＲＩ）は、セッショントラックの先頭（ディスクの内周側）にある領域で、セッションのＴＯＣ（Table OfContents：ＣＤに記録されているトラック数、開始位置およびデータ領域の合計の長さ）を保存する領域である。セッションをクローズすると、ＰＭＡに一時保存されていた情報がこのリードイン（ＲＩ）に書き込まれる。

【００１７】Ｔ５～Ｔ６に位置するデータエリア（ＵＡ）は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約６８０Ｍバイト（直径８ｃｍのものは最大約１９０Ｍバイト）であり、この記憶容量は録音時間で表すと最大約７４分（直径８ｃｍのものは最大約２１分）になる。データエリア（ＵＡ）は、リードイン（ＲＩ）のすぐ後ろから連続する所定サイズ（２Ｋバイト）単位の論理ブロックで管理されるようになっており、各論理ブロックごとに０から最大約３３０００までのＬＢＮ（Logical Block Number）が割り当てられるようになっている。Ｔ６～Ｔ７に位置するリードアウト（ＲＯ）は、セッションの最後（ディスクの外周側）にある領域で、データエリア（ＵＡ）の最後に到達したことを示す領域である。

【００１８】これら各領域のディスク上の位置はＴ３を除いて規格化されている。すなわち、Ｔ２はＴ０から２２．５ｍｍ離れた位置、Ｔ４はＴ０から２３ｍｍ離れた位置、Ｔ５はＴ０から２５ｍｍ離れた位置、Ｔ６はＴ０から５８ｍｍ離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト（ＲＯ）の終了位置とを同一の符号（Ｔ７）で示しているが、これは図示の都合である。リードアウト（ＲＯ）の実際の終了位置はＴ０から５８．５ｍｍ離れた位置になる。以下、特に断りのない限り、Ｔ７はリードアウト（ＲＯ）の終了位置を表すものとする。ちなみに、リードアウト（ＲＯ）の開始と終了位置（Ｔ６およびＴ７）はＣＤ－Ｒ１に記録するデータの量に応じて変化する。上記の実際値（Ｔ６＝５８ｍｍ、Ｔ７＝５８．５ｍｍ）は記憶データ量を最大にしたときのものである。

【００１９】図３は、ＣＤ－Ｒ１の断面構造図である。ＣＤ－Ｒ１は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性（屈折率や複屈折など）を備えた材料（例えばプラスチック）からなる基板１ｂの上に、有機色素からなる記録層１ｃ、アルミニウムなどの金属材料からなる反射層１ｄおよび樹脂等の硬質材料

からなる保護層１ｅを積層して形成されている。断面全体の厚さは１．２ｍｍである。

【００２０】ＣＤ－ＲＯＭとの構造上の相違は、記録層１ｃを有する点、および記録層１ｃと基板１ｂとの間にウォッブルグルーブと呼ばれる渦巻状の案内溝１ｆが形成されている点にある。ＣＤ－Ｒ１へのデータの記録は基板１ｂの裏側から案内溝１ｆに沿って記録用の強いレーザを照射し、記録層１ｃを加熱して情報ピット（Pit：再生用のレーザ反射光を変調するための物理的変形変質部分）を形成することにより行われる。案内溝１ｆは、ディスクの内周側から外周側（または外周側から内周側）に向かって一筆書きの要領で連続して形成されており、案内溝１ｆの幅は約０．５～０．７μｍ、間隔は約１．６μｍである。ユーザ段階におけるデータ記録は、案内溝１ｆに沿って、その案内溝１ｆ（または案内溝１ｆの間のランド部）直下の記録層１ｃに情報ピットを形成することによって行われる。なお、ＣＤ－Ｒ１の裏側から見て案内溝１ｆの凸部分をランド（山）、凹部分をグルーブ（谷）といい、一般に谷の部分をウォッブルグルーブというが、本明細書では山と谷を区別しない。

【００２１】ここで、案内溝１ｆの一の役割は、ユーザ段階のデータ記録時にディスクの回転速度を制御するためのタイミング情報を保持することにある。この役割のため、案内溝１ｆは、所定の周期（例えば２２．０５ｋＨｚに相当する周期）で蛇行（「ウォブリング」ともいう。）する形状に形成されている。データの記録時には、この蛇行を光ピックアップでトレースして周期を検出し、その検出周期が一定となるようにディスクの回転速度を制御することにより、データ記録時の光ピックアップとディスク間の相対速度を一定に保つ。案内溝１ｆの他の役割は、ディスク上の各記録領域（ＰＣＡ、ＰＭＡ、ＲＩ、ＵＡおよびＲＯ）の位置情報をはじめとした様々なディスク情報を保持することにある。ディスク情報はＡＴＩＰ（Absolute Time In Pregroove：通称「Ａチップ」という。）とも呼ばれており、ＡＴＩＰには、上記の位置情報のほかに、基準の記録レーザ強度やディスク回転速度、アプリケーションコードあるいはディスクタイプなどの各種情報が含まれている。

【００２２】図４は、ＣＤ－Ｒ１の各記録領域のフォーマット概念図である。この図において、ＰＣＡ、ＰＭＡ、リードイン（ＲＩ）、データエリア（ＵＡ）およびリードアウト（ＲＯ）はそれぞれ、図２（ｂ）における同名部分に対応する。ＰＣＡおよびＰＭＡのサイズ（情報書き込み可能容量）は特に決められていないが、前述の試し書き回数（一般に１００回程度）やセッション情報の一時記憶回数に見合った必要量、例えば、ＰＣＡで約３．５Ｍバイト程度、ＰＭＡで約２Ｍバイト程度の容量が確保されている。ちなみに、これらの例示容量からＰＣＡの開始位置（Ｔ２）とＰＭＡの開始位置（Ｔ３）は、規格化されたリードイン（ＲＩ）の開始位置（Ｔ４）を基準として、「Ｔ２＝Ｔ４－約３５秒」の位置、「Ｔ３＝Ｔ４－約１３秒」の位置と書き表すことができる。

【００２３】既述のとおり、ＰＣＡはデータ記録を行う際の試し書き領域、ＰＭＡはクローズされていないセッション情報を一時的に格納する領域であるから、これら二つの領域（ＰＣＡ／ＰＭＡ）はデータ記録時にのみ利用（アクセス）される領域である。一方、リードイン（ＲＩ）はクローズされたセッション情報をＴＯＣとして記録する領域、データエリア（ＵＡ）は実際にデータが書き込まれる領域、リードアウト（ＲＯ）はデータエリアの終わりを明示する領域であるから、これら三つの領域（リードイン／データエリア／リードアウト）はデータ記録時と再生時の両方で利用（アクセス）される領域である。

【００２４】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、ＣＤ－Ｒ１の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール（典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど）を用いて容易にアクセスできるか否かの点で評価すると、データエリア（ＵＡ）については当然ながらその記憶内容の全容把握は可能であるが、他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）の内容把握は不可能である。

【００２５】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるため、かかる例外的なツールの利用を除けば、データエリア以外の他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）は、システムからのアクセスだけが許可された特殊な領域であるということができる。本明細書では、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」という。すなわち、データエリア（ＵＡ）はユーザ領域、それ以外のＰＣＡ、ＰＭＡ、リードイン（ＲＩ）およびリードアウト（ＲＯ）はシステム領域である。

【００２６】本実施の形態におけるＣＤ－Ｒ１は、先に説明したとおり、製造段階でシステム領域の一部にＣＤ－Ｒ１の固有情報（以下「ＩＤ情報」という。）と所定の暗号鍵情報とが書き込まれる。ＩＤ情報はＣＤ－Ｒ１の全製造数にわたってユニークな値（重複しない値）を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。

【００２７】このＩＤ情報は、後述するように、ユーザ段階でのＣＤ－Ｒ１へのアクセス照合に用いられる。例

えば、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（ＩＤを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【００２８】ＣＤ－Ｒ１に書き込まれたＩＤ情報のユーザへの通知は、各々のＣＤ－Ｒ１の購入者（または正規入手者）ごとに行わなければならない。例えば、あるＣＤ－Ｒ１（以下、便宜的に「ディスクＡ」とする。）に書き込まれたＩＤ情報を“ａｂｃｄｅｆ”と仮定すると、ディスクＡの購入者または正規入手者に対し、当該ＩＤ情報（“ａｂｃｄｅｆ”）を書面ないしその他の手段で通知する。この手段としては、例えば、ディスクＡのパッケージ（ディスクＡを収めたプラスチックケース）の中に当該ＩＤ情報（“ａｂｃｄｅｆ”）を記載した紙片を入れておいてもよいし、ディスクＡの購入時等に口頭で伝えてもよい。その他いろいろな手段が考えられるが、要は、出荷時にＣＤ－Ｒ１に書き込んだＩＤ情報をユーザに正確に伝達できればよい。

【００２９】一方、製造段階でシステム領域に一緒に書き込まれる鍵情報は、ユーザ段階でデータエリアに書き込まれる生データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをＣＤ－Ｒ１のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【００３０】したがって、ＩＤを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【００３１】図5は、システム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。この図において、第一の例（ａ）は、８バイトのＩＤ情報、８バイトのＤＥＳ（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で２０バイトの大きさを有している。また、第二の例（ｂ）は、８バイトのＩＤ情報、２４バイトのトリプルＤＥＳ暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で３６バイトの大きさを有している。いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構造はあくまでも例示である。要はＣＤ－Ｒ１の固体識別が可能な情報（ＩＤ情報）と、生データを暗号化データに変換できる共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とをＣＤ－Ｒ１のシステム領域に書き込んでおけばよい。

【００３２】図6は、ライトワンス型光ディスク記録再生装置（以下「ＣＤ－Ｒ記録再生装置」という。）の概略的なブロック構成図である。このＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のクランピングエリア（図２（ａ）のＴ１～Ｔ２の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ１２と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに記録用または再生用のレーザ（一般に波長７７０～８３０ｎｍの赤外レーザ）１３を照射する光ピックアップ１４と、光ピックアップ１４の内部に設けられた不図示のシークモータと協調して光ピックアップ１４をディスクの半径方向に移動させる粗動モータ１５とを備えると共に、スピンドルモータ１２の回転速度を制御するディスク回転制御部１６と、粗動モータ１５の回転速度と回転方向を制御する粗動モータ制御部１７と、光ピックアップ１４の位置やレーザ強度の制御を行うピックアップ制御部１８と、光ピックアップ１４からの読み取り信号や光ピックアップ１４への書き込み信号の波形変換等の制御を行う再生／記録制御部１９とを備え、さらに、これらの各制御部を統括するコントローラ２０を備える。

【００３３】ＣＤ－Ｒ記録再生装置１０は、パーソナルコンピュータ等のホスト装置２１の拡張スロットに内蔵され（または外付けされ）、ホスト装置２１とコントローラ２０との間を所定の信号規格（例えば、ＳＣＳＩ：Small Computer System Interface）のケーブル２１ａで接続して用いられる。

【００３４】このような構成を有するＣＤ－Ｒ記録再生装置１０は、以下に示すとおり、ＣＤ－Ｒ１への情報の記録とその記録情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ記録再生装置１０は、ＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００３５】＜ＣＤ－Ｒ１への情報の記録動作＞ホスト装置２１でＣＤ－Ｒ記録専用アプリケーションプログラム（以下「ライティングプログラム」という。）を実行すると、まず、ライティングプログラムからのレーザ強度キャリブレーションコマンドがコントローラ２０に伝

えられる。コントローラ２０はこのコマンドに応答して各制御部に所要の指令を伝え、光ピックアップ１４をＣＤ－Ｒ１のＰＣＡ空領域（試し書きされていない領域）に位置させると共に、スピンドルモータ１２の回転速度を制御（光ピックアップ１４の現在位置における相対速度が所定速度となるように制御）した後、光ピックアップ１４から暫定強度（５．５～８ｍＷの間の任意パワー）の記録用レーザ１３をＰＣＡ空領域に照射して試し書きを行う。光ピックアップ１４の位置制御およびスピンドルモータ１２の回転速度制御は、ＣＤ－Ｒ１の案内溝１ｆのトレース信号から再生された情報（タイミング情報およびＡＴＩＰ情報）に従って行われる。

【００３６】次いで、コントローラ２０は、再生／記録制御部１９を介してＰＣＡに試し書きされたデータを読み取り、そのデータをホスト装置２１のライティングプログラムに返送する。ライティングプログラムは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が“否”であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が“適”であれば、ＣＤ－Ｒ１への情報の記録動作を開始する。

【００３７】この記録動作は、ユーザによって適宜に選択された所要の記録データをライティングプログラムからコントローラ２０に伝え、このコントローラ２０の制御の下、各制御部を介してスピンドルモータ１２の回転制御および光ピックアップ１４の位置制御を行いつつ、上記記録データで光ピックアップ１４からの記録用レーザ１３を変調しながらＣＤ－Ｒ１のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のＴＯＣをリードイン（ＲＩ）に書き込むと共に、最終セッションの後にリードアウト（ＲＯ）を形成する。

【００３８】＜ＣＤ－Ｒ１の記録情報の再生動作＞ＣＤ－Ｒ１の記録情報を再生する際に上記ライティングプログラムは不要である。但し、ＣＤ－Ｒ１のファイルシステムとホスト装置２１のファイルシステムとの相互変換を行うためのドライバソフトの類は必須である。ユーザはこのドライバソフトを介してＣＤ－Ｒ記録再生装置１０を利用することにより、ホスト装置２１に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにＣＤ－Ｒ１のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でＣＤ－Ｒ１内の目的とするファイルを利用することができるようになっている。

【００３９】ＣＤ－Ｒ記録再生装置１０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置２１のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ１４を位置させると共に、スピンドルモータ１２の回転速度を制御し、光ピックアップ１４から再生用のレーザ（パワーが０．２ｍＷ程度に抑えられる点を除き記録用のレーザと同じもの）１３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置２１に転送するという一連の動作を実行する。

【００４０】このように、ＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１への情報の書き込みを行うことができると共に、ＣＤ－Ｒ１に書き込まれた情報の再生も行うことができる。このＣＤ－Ｒ記録再生装置１０は、記録段階でＣＤ－Ｒ１への情報の書き込みを行う場合に必要不可欠な構成要素であるが、再生段階で、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合も必要とされる構成要素である。ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはＣＤ－ＲＯＭ再生装置が搭載されており、そのＣＤ－ＲＯＭ再生装置を利用してＣＤ－Ｒ１の情報再生を行うことも可能であるが、このＣＤ－ＲＯＭ再生装置は、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報や暗号鍵にアクセスできないから、やはり、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合もＣＤ－Ｒ記録再生装置１０は欠かせない構成要素である。

【００４１】また、ＣＤ－Ｒ記録再生装置１０はもっぱらユーザによる記録や再生で使用される装置であるが、ＣＤ－Ｒ１への情報書き込み機能に注目すると、その基本的動作は、ＣＤ－Ｒ１の製造段階で行われるＩＤ情報や暗号鍵の書き込みにも適用可能であるから、以下の説明では上記のＣＤ－Ｒ記録再生装置１０をユーザ段階と製造段階の両方で使用されるものとして話を進める。

【００４２】＜出荷時情報記録処理＞図７は、ＣＤ－Ｒ１の製造段階におけるＩＤ情報と暗号鍵の書き込み動作（以下「出荷時情報記録処理」という。）を示すフローチャートである。なお、製造段階では、ＣＤ－Ｒ記録再生装置１０の記録機能しか利用しないため、図示のフローチャートではＣＤ－Ｒ記録再生装置１０のことを便宜的に「記録機」と称している。但し、この用語（記録機）には、ＣＤ－Ｒ記録再生装置１０に限らず、製造段階専用の“記録機”であってもよい旨の意図も含まれている。

【００４３】図において、出荷時情報記録処理を開始すると、まず、未記録のＣＤ－Ｒ１（フロー中では「ディスク」と称する。）を用意し、このＣＤ－Ｒ１を記録機に装填する（ステップＳ１１）。次に、ホスト装置２１を操作してＣＤ－Ｒ１への記録情報を手入力または自動生成する（ステップＳ１２）。この記録情報はＣＤ－Ｒ１のＩＤ情報や所定の秘密鍵および当日の日付（作成日

付）などであり、そのフォーマットは、図5（ａ）または（ｂ）に示すとおりである。

【００４４】次いで、ホスト装置２１から記録機に対して情報記録命令を発行すると（ステップＳ１３）、記録機はこの命令に応答してレーザ強度キャリブレーション処理を実行し、適正なパワーに記録用レーザ１３を設定した後、光ピックアップ１４をＣＤ－Ｒ１の記録領域の“特定位置”に移動制御する（ステップＳ１４）。この特定位置は原理的にはユーザからの直接的なアクセスが認められていない領域、すなわち、システム領域（ＰＣＡ、ＰＭＡ、リードインまたはリードアウト）の未使用領域上の任意位置である。特に好ましくは、データ再生時にその存在が無視される領域として当業者に広く認知されているＰＣＡまたはＰＭＡ上の（未使用領域上の）任意位置である。以下、説明の便宜上、上記“特定位置”をＰＣＡの未使用領域上の任意位置とする。

【００４５】次いで、記録機は、ホスト装置２１から記録情報（ステップＳ１２で生成した情報）を受け取り、その記録情報を用いて記録用レーザ１３を変調しつつ、記録用レーザ１３をＣＤ－Ｒ１の透明な基板１ｂを介して記録層１ｃの案内溝１ｆに照射し、案内溝１ｆ直下の記録層１ｃに情報ピットを形成して、前記記録情報のＣＤ－Ｒ１への書き込みを行う（ステップＳ１５）。記録情報の書き込み開始位置は、上記ステップＳ１４で実行された光ピックアップ１４の移動位置、すなわち、ＰＣＡの未使用領域上の任意位置であり、記録情報の書き込み終了位置は当該位置から記録情報のサイズ（例えば、図5のフォーマットに従えば２０バイトまたは３６バイト）に相当する分だけ離れた位置である。

【００４６】次いで、記録機は、光ピックアップ１４を上記特定位置に復帰させると共に、当該位置を再生開始位置、記録情報のサイズに相当する分だけ離れた位置を再生終了位置として、システム領域に書き込んだ記録情報の再生を行い、この再生情報をホスト装置２１に転送する。ホスト装置２１は、記録機から転送された再生データと上記記録情報とを比較照合してベリファイ検査を行い（ステップＳ１６）、両者が一致していれば正常に書き込みを行えたと判断してその旨を作業者に報知する一方、そうでなければ書き込みを失敗したと判断してその旨を作業者に報知する（ステップＳ１７）。作業者は、正常書き込み報知の場合に当該ＣＤ－Ｒ１を出荷棚へ移動し（ステップＳ１８）、書き込み失敗報知の場合に当該ＣＤ－Ｒ１を不良品棚へ移動する（ステップＳ１９）。そして、以上の処理を用意されたＣＤ－Ｒ１がなくなるまで繰り返して実行する（ステップＳ２０）。

【００４７】したがって、この「出荷時情報記録処理」によれば、未記録のＣＤ－Ｒ１のシステム領域にＩＤ情報、暗号鍵および作成日付などの隠し情報を書き込んで市場に出荷し、ユーザに届けることができる。そして、ユーザ段階で、以下に説明するデータ書き込み処理、データ再生処理またはディスクコピー処理を行う際に、上記の隠し情報を利用した本実施の形態特有の処理を実行することができる。

【００４８】＜ユーザによるデータ書き込み処理＞図8は、ユーザ段階で実行されるデータ書き込み動作（以下「ユーザによるデータ書き込み処理」という。）を示すフローチャートである。ユーザは上述の「出荷時情報記録処理」を終えたＣＤ－Ｒ１を市場で入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０にセットして、図示の処理を開始する。

【００４９】この処理を開始すると、まず、ホスト装置２１からＣＤ－Ｒ記録再生装置１０へ書き込み命令が発行される。ＣＤ－Ｒ記録再生装置１０はこの命令に応答してＣＤ－Ｒ１のシステム領域からＩＤ情報を読み出し（ステップＳ３１）、サポートディスクであるか否かを判定する（ステップＳ３２）。サポートディスクとは、前述のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたディスクのことである。ＣＤ－Ｒ記録再生装置１０はこれらの製造者を識別するためのＩＤ情報リスト（以下「サポートリスト」という。）を保持しており、上記のステップＳ３２で当該サポートリストを参照してＩＤ情報が登録済みであれば、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクであると判定する。

【００５０】ステップＳ３２の判定結果が“否”（ＮＯ）の場合、すなわち、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクでない場合は、ホスト装置２１に対してサポートディスクへの交換を促す旨のメッセージ（例えば、“このディスクはセキュリティ対応ではありません。セキュリティ対応のディスクに交換してください。”）を送出（ステップＳ３３）して、ディスク交換後の書き込み続行または書き込み中止を判定（ステップＳ３８）する一方、ステップＳ３２の判定結果が“肯”（ＹＥＳ）の場合、すなわち、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクである場合は、以下の処理を実行する。

【００５１】まず、記録データに機密フラグを付加する（ステップＳ３４）。この機密フラグは、前述のとおり、再生段階において、復号後の平文データの再利用を禁止するためのチェックフラグとして用いられるものであり、好ましくは、電子透かしのような技術を応用してその存在を秘匿化したデータのことである。次いで、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１のシステム領域から暗号鍵を読み出し（ステップＳ３６）、その暗号鍵を用いて上記の機密フラグを付加した記録データを暗号化した後、その暗号化データをＣＤ－Ｒ１のユーザ領域に記録する（ステップＳ３７）。

【００５２】最後に、他のＣＤ－Ｒ１に書き込みを行うか否かを判定し（ステップＳ３８）、書き込みを継続す

る場合は、所要のメッセージ（例えば、“新しいディスクをセットしてください”）をホスト装置２１に送出すると共に、書き込み済みのＣＤ－Ｒ１をリジェクトしてステップＳ３１以降を繰り返し、書き込みを継続しない場合は書き込み済みのＣＤ－Ｒ１をリジェクトして処理を終了する。

【００５３】図９は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図である。この図において、ユーザは、ＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０に装填すると共に、ホスト装置２１を操作して所要の書き込み命令をＣＤ－Ｒ記録再生装置１０に発行する。ＣＤ－Ｒ記録再生装置１０はこの書き込み命令に応答して、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報を読み出し、所定のＩＤ情報リスト（サポートリスト）と照合してサポートディスクであるか否かを判定する。そして、サポートディスクでなければ、ホスト装置２１に対してディスクの交換を促し、サポートディスクであれば、ホスト装置２１に対してその旨を通知する。ホスト装置２１はサポートディスクである旨の通知に応答して、記録データに機密フラグを付加し、ＣＤ－Ｒ記録再生装置１０に対して暗号鍵を要求する。ＣＤ－Ｒ記録再生装置１０はＣＤ－Ｒ１のシステム領域から暗号鍵を読み出し、その暗号鍵をホスト装置２１に転送する。ホスト装置２１は転送された暗号鍵を用いて記録データ（機密フラグを付加したもの）を暗号化し、その暗号化データをＣＤ－Ｒ記録再生装置１０に転送し、ＣＤ－Ｒ記録再生装置１０は転送された暗号化データをＣＤ－Ｒ１に記録する。

【００５４】したがって、この「ユーザによるデータ書き込み処理」によれば、所定のサポートリストに記載されたＩＤ情報を持つＣＤ－Ｒ、要するに、特定の製造者によって作られたＣＤ－Ｒについてのみ、そのユーザ領域に、機密フラグを付加した記録データを暗号化して記録することができるから、サポートリストに未記載の製造者によって作られたＣＤ－Ｒとの差別化を図ることができ、市場での優位性を得ることができる。

【００５５】＜ユーザによるデータ再生処理＞図１０は、ユーザ段階のデータ再生に用いられる再生専用機（以下「ＣＤ－Ｒ再生装置」という。）の概略的なブロック構成図であり、前述のＣＤ－Ｒ記録再生装置１０（図６参照）との相違は、データの記録機能を持たない点である。すなわち、このＣＤ－Ｒ再生装置３０（発明の要旨に記載のライトワンス型光ディスク用データ再生装置に相当）は、ＣＤ－Ｒ１のクランピングエリアを担持して所定方向に回転駆動するスピンドルモータ３２と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに再生用のレーザ３３を照射する光ピックアップ３４と、光ピックアップ３４の内部に設けられた不図示のシークモータと協調して光ピックアップ３４をディスクの半径方向に移動させる粗動モータ３５とを備えると共に、スピンドルモータ３２の回転速度を制御するディスク回転制御部３６と、粗動モータ３５の回転速度と回転方向を制御する粗動モータ制御部３７と、光ピックアップ３４の位置やレーザ強度の制御を行うピックアップ制御部３８と、光ピックアップ３４からの読み取り信号の波形変換等の制御を行う再生制御部３９とを備え、さらに、これらの各制御部を統括するコントローラ４０を備える。

【００５６】このＣＤ－Ｒ再生装置３０は、前述のＣＤ－Ｒ記録再生装置１０と同様に、パーソナルコンピュータ等のホスト装置５１の拡張スロットに内蔵され（または外付けされ）、ホスト装置５１とコントローラ４０との間を所定の信号規格（例えば、ＳＣＳＩ）のケーブル５１ａで接続して用いられる。

【００５７】このような構成を有するＣＤ－Ｒ再生装置３０は、以下に示すとおり、ＣＤ－Ｒ１に書き込まれた情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ再生装置３０は、先に説明したＣＤ－Ｒ記録再生装置１０と同様にＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００５８】図１１は、ホスト装置５１の階層的機能概念図であり、図示の階層構造は、いわゆるＯＳＩ（Open System Interconnection：開放型システム間相互接続）参照モデルと同様に最下位層を物理層、最上位層をアプリケーション層とする構造を有している。この構造は大きく分けて、物理層と密接に関係するドライバ層５１ｂと、その上位に位置するいわゆるオペレーティングシステム（ＯＳ）によって提供されるサービス層５１ｃと、最上位層に位置してユーザインターフェースを実現するためのアプリケーション層５１ｄとからなり、アプリケーション層５１ｄに実装されたアプリケーションプログラム（例えば、ＣＤ－Ｒ再生装置３０を利用するためのユーザインターフェースを含むもの）５１ｅは、サービス層５１ｃのオペレーティングシステム５１ｆのＡＰＩ（Application Programmable Interface）を介してドライバ層５１ｂにアクセスし、例えば、ＣＤ－Ｒ再生装置３０をはじめとした各種リソースを利用する。

【００５９】ここで、ドライバ層５１ｂには多種多様なドライバプログラムが実装されている。例えば、ＣＤ－Ｒ再生装置３０のインターフェース規格をＳＣＳＩとすると、少なくともＳＣＳＩドライバ（ＡＴＡＰＩドライバともいう）５１ｇやＳＣＳＩポート用のミニポートドライバ５１ｈおよび入出力制御用のＩＯＳ（Input/Output Supervisor）ドライバ５１ｉなどが実装されている。

【００６０】一般にアプリケーションプログラム５１ｅはオペレーティングシステム５１ｆの所定のＡＰＩを利用して、物理層に位置する各種リソースを利用するが、通常、アプリケーションプログラム５１ｅから見て、これらのドライバの存在は意識されない。例えば、アプリ

ケーションプログラム５１ｅからＣＤ－Ｒ再生装置３０を利用する場合、実際には、ＩＯＳドライバ５１ｉやＳＣＳＩドライバ５１ｇおよびミニポートドライバ５１ｈを間接的に利用している。また、ファイルコピーの操作などを行う場合も、実際にはＩＯＳドライバ５１ｉを間接的に利用している。

【００６１】ところで、図示のドライバ層５１ｂには、ハッチングで他と区別された特別なドライバ（以下「フィルタドライバ」という。）５１ｊが実装されている。このフィルタドライバ５１ｊは本実施形態に特有のもので、少なくとも（ａ）アプリケーションプログラム５１ｅの要求に応じてＣＤ－Ｒ再生装置３０からオペレーティングシステム５１ｆに渡されるデータをモニタし、そのデータ内に前述の“機密フラグ”が含まれているか否かを判定する第一の機能と、（ｂ）上記“機密フラグ”の存在を判定した場合に当該データに対するオペレーティングシステム５１ｆのコピー動作や保存動作を拒否ないしは制限（例えば、コピー命令や保存命令を無視したりすること）する第二の機能とを持つものであり、発明の要旨に記載の判定手段および禁止手段に相当するものである。

【００６２】第一の機能を実現するために、フィルタドライバ５１ｊはＳＣＳＩドライバ５１ｇとミニポートドライバ５１ｈの間に実装されており、さらに、第二の機能を実現するために、オペレーティングシステム５１ｆとＩＯＳドライバ５１ｉの間に実装されている。なお、この実装位置は一例である。要はアプリケーション層５１ｄから直接的にアクセスできない位置であって、且つ、上記モニターと上記コピー動作や保存動作の拒否に適した位置に実装されていればよい。また、フィルタドライバ５１ｊは図示のように単一のものでなく、各機能ごとに分割されたものであってもよい。

【００６３】ユーザは、アプリケーションプログラム５１ｅによって提供されるユーザインターフェースを操作しながらＣＤ－Ｒ再生装置３０にアクセスし、ＣＤ－Ｒ１に記録されたデータの再生を行う。この再生処理に際して、オペレーティングシステム５１ｆやドライバプログラム５１ｇ～５１ｊは黒子的な仲介役となって表に出てこない。すなわち、ユーザは、オペレーティングシステム５１ｆやドライバプログラム５１ｇ～５１ｊの存在を意識することなく、ＣＤ－Ｒ再生装置３０にアクセスし、ＣＤ－Ｒ１に記録されたデータを利用することができる。

【００６４】ＣＤ－Ｒ１に記録されたデータは、アプリケーションプログラム５１ｅから見て、オペレーティングシステム５１ｃのファイルシステムによって管理された独立したデータの集まり（ファイル）として認識される。ユーザは、このデータを他の記憶デバイスに格納されたデータと同様に取り扱う（ファイルアクセス）ことができる。ＣＤ－Ｒ再生装置３０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置５１のドライバ層５１ｂに提供すると共に、当該ドライバソフト層５１ｂから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ３４を位置させると共に、スピンドルモータ３２の回転速度を制御し、光ピックアップ３４から再生用のレーザ３３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置５１のドライバ層５１ｂに転送するという一連の動作を実行する。

【００６５】図１２は、ユーザ段階で実行されるデータ再生動作（以下「ユーザによるデータ再生処理」という。）を示すフローチャートである。ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ再生装置３０にセットして、そのＣＤ－Ｒ１からＩＤ情報を読み出す（ステップＳ４１）と共に、ホスト装置５１に対してＩＤ入力を要求する（ステップＳ４２）。ホスト装置５１は、画面上にＩＤ入力を促す旨の所定のＧＵＩ（Graphical User Interface）を表示してユーザによるキーボード等からのＩＤ入力を受け付け、入力されたＩＤ情報をＣＤ－Ｒ記録再生装置１０に転送する。ＣＤ－Ｒ再生装置３０は、転送されたＩＤ情報とＣＤ－Ｒ１から読み込んだＩＤ情報とを比較し（ステップＳ４３）、一致した場合は正規ユーザ、一致しなかった場合は不正なユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、以下の処理を実行する。

【００６６】まず、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵と暗号化データを読み出して（ステップＳ４４、ステップＳ４５）、ホスト装置５１に転送する。ホスト装置５１は、転送されたデータに機密フラグが含まれているか否かを判定し（ステップＳ４６）、含まれている場合は、暗号鍵を用いてその暗号化データを復号し（ステップＳ４７）、平文のデータに戻してユーザの利用に供する一方、機密フラグが含まれていない場合は、復号動作を行うことなく、そのまま処理を終了する。

【００６７】図１３は、上記「ユーザによるデータ再生処理」のタイムランを示す図である。この図において、ユーザは、ＣＤ－Ｒ１をＣＤ－Ｒ再生装置３０に装填すると共に、ホスト装置５１を操作して所要の再生命令をＣＤ－Ｒ再生装置３０に発行する。ＣＤ－Ｒ再生装置３０はこの再生命令に応答してＩＤ要求をホスト装置５１に返し、ホスト装置５１は画面上にＩＤ入力を促す旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ１の配布先から正当に通知された

ＩＤ情報）を入力し、ホスト装置５１は入力されたＩＤ情報をＣＤ－Ｒ再生装置３０に転送する。

【００６８】ＣＤ－Ｒ再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出し、ホスト装置５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置５１に転送する。ホスト装置５１は、転送データ中に機密フラグがあるか否かを判定し、機密フラグが含まれている場合は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容する一方、機密フラグが含まれていない場合は復号動作を行うことなく、処理を終了する。

【００６９】したがって、この「ユーザによるデータ再生処理」によれば、ＣＤ－Ｒのシステム領域に書き込まれているＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができ、正規ユーザによってデータ再生処理が行われている場合に、ＣＤ－Ｒのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送することができる。そして、転送データ中に機密フラグが含まれている場合に、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を当該正規ユーザに許容することができる。

【００７０】その結果、不正ユーザを排除してデータの再生を行うことができると共に、機密フラグが含まれている暗号化データの復号のみを行うことができるから、前記の「ユーザによるデータ書き込み処理」との組み合わせによって、記録段階から再生段階までの一連のセキュリティ対策を確立することができるうえ、このセキュリティ対策に欠くことのできない記録媒体として特定の製造者によって作られたサポートディスクの使用を強制することができる。

【００７１】＜ユーザによるディスクコピー処理＞図１４は、ユーザ段階で実行されるデータコピー動作（以下「ユーザによるデータコピー処理」という。）を示すフローチャートである。なお、以下の説明では、データのコピー先をＣＤ－Ｒとしているが、これはデータ再利用の一例であり、コピー先は如何なる記憶媒体であってもかまわない。ハードディスクやその他の記録媒体であってもよい。

【００７２】図１４において、ユーザによるデータコピー処理を開始すると、ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたＣＤ－Ｒ１をコピー元、未記録のＣＤ－Ｒをコピー先とし、それぞれをコピー元のＣＤ－Ｒ再生装置３０とコピー先のＣＤ－Ｒ記録再生装置１０にセットする。そして、ホスト装置５１を操作してコピー元のＣＤ－Ｒ再生装置３０にコピー命令を発行する。コピー元のＣＤ－Ｒ再生装置３０は、コピー命令に応答してＣＤ－Ｒ１からＩＤ情報を読み出す（ステップＳ５１）と共に、ホスト装置５１に対してＩＤ入力を要求する（ステップＳ５２）。ホスト装置５１は画面上にＩＤ入力を促す旨の所定のＧＵＩを表示してユーザによるキーボード等からのＩＤ入力を受け付け、入力されたＩＤ情報をコピー元のＣＤ－Ｒ再生装置３０に転送する。

【００７３】コピー元のＣＤ－Ｒ再生装置３０は、転送されたＩＤ情報とＣＤ－Ｒ１から読み込んだＩＤ情報とを比較し（ステップＳ５３）、一致した場合は正規ユーザ、一致しなかった場合は不正ユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、コピー元のＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵と暗号化データを読み出してホスト装置５１に転送する。ホスト装置５１は、そのドライバ層５１ｂに実装されたフィルタドライバ５１ｊにより、転送データ中に機密フラグが存在するか否かを判断し（ステップＳ５４）、機密フラグが存在しなければ、転送された暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のＣＤ－Ｒ記録再生装置１０に転送してコピー先のＣＤ－Ｒ１に記録するというコピー処理を実行（ステップＳ５５）して処理を終了する一方、機密フラグが存在していれば、同コピー処理を強制的に中止（ステップＳ５６）して処理を終了する。

【００７４】図１５は、上記「ユーザによるデータコピー処理」のタイムランを示す図であり、図中のＣＤ－Ｒ１とＣＤ－Ｒ再生装置３０はコピー元のもの、ＣＤ－Ｒ記録再生装置１０とＣＤ－Ｒ１′はコピー先のものである。この図において、ユーザは、コピー元とコピー先のＣＤ－Ｒ１、１′をそれぞれＣＤ－Ｒ再生装置３０とＣＤ－Ｒ記録再生装置１０に装填すると共に、ホスト装置５１を操作して所要のコピー命令をコピー元のＣＤ－Ｒ再生装置３０に発行する。コピー元のＣＤ－Ｒ再生装置３０はこのコピー命令に応答してＩＤ要求をホスト装置５１に返し、ホスト装置５１は画面上にＩＤ入力を促す旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ１の配布先から正当に通知されたＩＤ情報）を入力し、ホスト装置５１は入力されたＩＤ情報をコピー元のＣＤ－Ｒ再生装置３０に転送する。

【００７５】コピー元のＣＤ－Ｒ再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出し、ホスト装置５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を終了する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ１に書き込まれている暗号鍵と暗号化データとを読み出してホスト装置５１に転送する。ホスト装置５１は、そのドライバ層５１ｂに実装されたフィルタ

ドライバ51jにより、転送データ中の機密フラグの存在を判断する。そして、存在していればコピー処理を強制的に中止する一方、存在していなければ、暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のCD-R記録再生装置10に転送し、コピー先のCD-R記録再生措置10はその転送データをCD-R1′に書き込む。

【0076】したがって、この「ユーザによるデータコピー処理」によれば、コピー元のCD-Rのシステム領域に書き込まれているID情報を用いて正規ユーザと不正ユーザとを識別することができると共に、機密フラグが付加されたデータのコピーが行われようとした場合は、たとえ正規ユーザであっても、そのコピー動作を強制的に中止（コピー動作の拒否）して実行しないようにすることができる。その結果、暗号化データに機密フラグが存在する場合は、コピー処理を積極的に禁止できるから、復号データの再利用を阻止することができ、記録から再生までのすべての段階にわたってセキュリティを持たせることができる。

【0077】<まとめ>以上、説明したとおり、本実施の形態によれば、CD-R1のシステム領域に書き込まれたID情報を用いて、サポートリストに記載された製造者のCD-R1（サポートディスク）であるか否かを判定でき、サポートディスクの場合に所定の機密フラグを付加した記録データを暗号化してCD-R1に記録することができる。そして、再生側でこの暗号化データを読み出す際に、機密フラグの有無を検査し、機密フラグがある場合に復号データの再利用を禁止することができる。したがって、ホスト装置51の内部には、前述の「ユーザによるデータ再生処理」によってメインメモリ上に一時的に作られた復号データしか存在しないため、しかも、この一時的データはプロセスからの利用完了時点で速やかに解放されるため、再利用可能な復号データの痕跡が残されることはなく、データの不正流出等を確実に防止することができるという格別有益な効果が得られる。

【0078】なお、以上の説明では、ID情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のPCAやPMAはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【0079】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のDES方式以外にも、FEAL：Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバヘッドおよび暗号化データのボリューム等を勘案して適切な方式を採用すればよい。

【0080】また、前記説明のセキュリティ機能のうち、特に復号データの再利用を禁止する機能は、もっぱらホスト装置51に実装されたフィルタドライバ51jやその他の汎用ドライバおよびオペレーティングシステム等のソフトウェアリソースと、ホスト装置51の各種ハードウェアリソースとの有機的結合によって機能的に実現されるものであるが、フィルタドライバ51j以外のリソースは汎用のものを利用できるから、前記説明の「復号データの再利用を禁止する機能」にとって欠くことのできない必須の事項は、実質的に、フィルタドライバ51jのプログラムに集約されているということがいえる。したがって、本発明に係るセキュリティ機能のポイントは、それらのプログラムのすべてまたはその要部を格納した、フロッピィディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む構成品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または構成品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

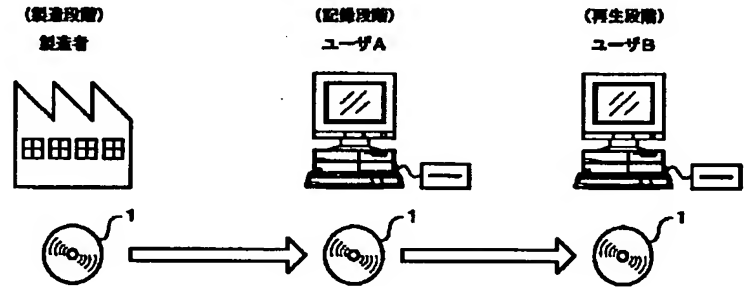
【0081】また、以上の説明では、ライトワンス型光ディスクとしてCD-Rの例を示したが、これに限らない。例えば、DVD（Digital Video DiscまたはDigital Versatile Disc）-Rも1回だけのデータ書き込みを行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をDVD-Rに適用する場合、CD-RをDVD-Rと読み替えると共に、CD-R記録再生装置やCD-RライターをそれぞれDVD-R記録再生装置、DVD-Rライターと読み替えればよい。

【0082】

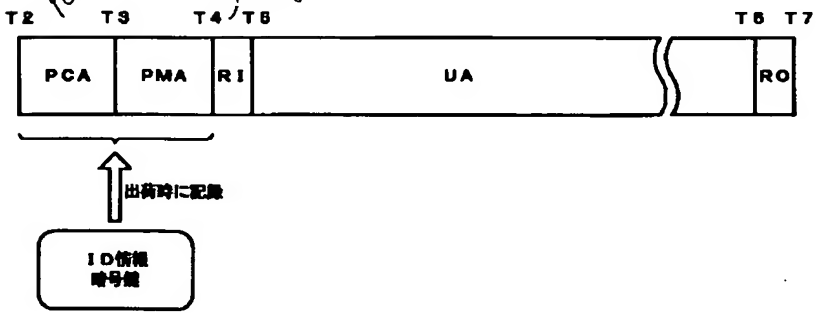
【発明の効果】請求項1記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が制限される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項2記載の発明によれば、光ディスクのシステム領域に不可視状態で格納されたセキュリティ情報に基づいて光ディスクへのアクセスが制限される。したがって、例えば、データ再生時に正当なユーザを認証して書き込みデータへのアクセスを許容することができ、不正ユーザの排除等、セキュリティ性の向上を図ることができる。請求項3記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が禁止される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項4記載の発明によれば、マイクロコンピュータを含むハードウェアリソースと該プログラムとの有機的結合によって前記判定手段および禁止手段を実現できる。

【図面の簡単な説明】
【図1】本実施形態のCD-Rの利用模式図である。
【図2】ライトワンス型光ディスクの外観図およびその要部拡大図である。
【図3】CD-Rの断面構造図である。
【図4】CD-Rの各記録領域のフォーマット概念図である。
【図5】CD-Rのシステム領域に書き込まれるID情報と暗号鍵を含むデータフォーマットの例示構造図である。
【図6】CD-R記録再生装置の概略的なブロック構成図である。
【図7】出荷時情報記録処理を示すフローチャートである。
【図8】ユーザによるデータ書き込み処理を示すフローチャートである。
【図9】ユーザによるデータ書き込み処理のタイムランを示す図である。
【図10】CD-R再生装置の概略的なブロック構成図である。
【図11】ホスト装置の階層的機能概念図である。
【図12】ユーザによるデータ再生処理を示すフローチャートである。
【図13】ユーザによるデータ再生処理のタイムランを示す図である。
【図14】ユーザによるディスクコピー処理を示すフローチャートである。
【図15】ユーザによるディスクコピー処理のタイムランを示す図である。
【図16】従来のセキュリティ対策の概念図である。
【符号の説明】
PCA　Power Calibration Area（システム領域）
1　CD-R（ライトワンス型光ディスク）
30　CD-R再生装置（ライトワンス型光ディスク用データ再生装置）
51j　フィルタドライバ（判定手段、禁止手段）

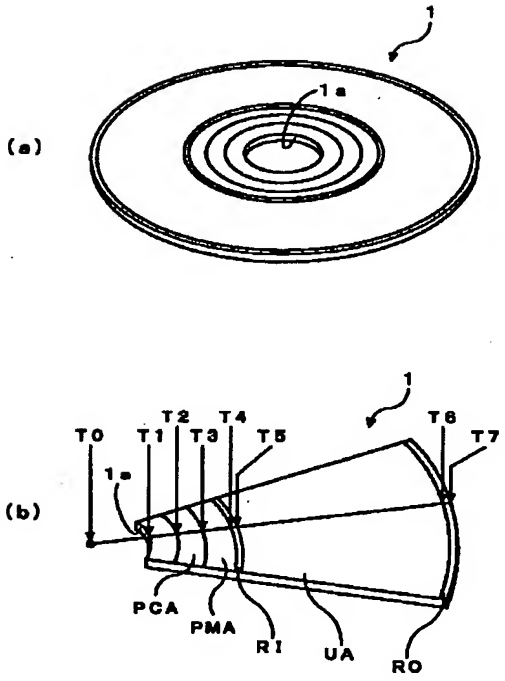
【図1】



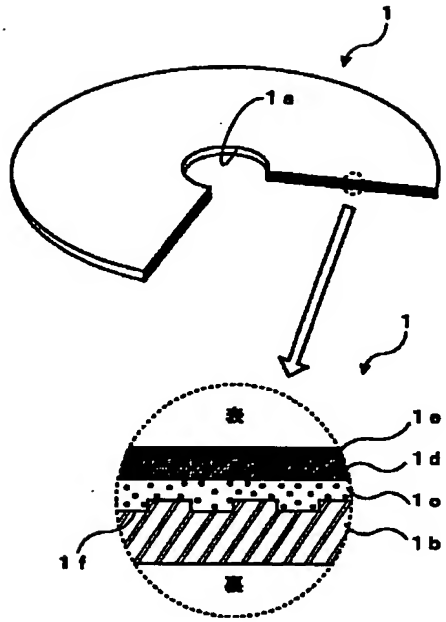
【図4】



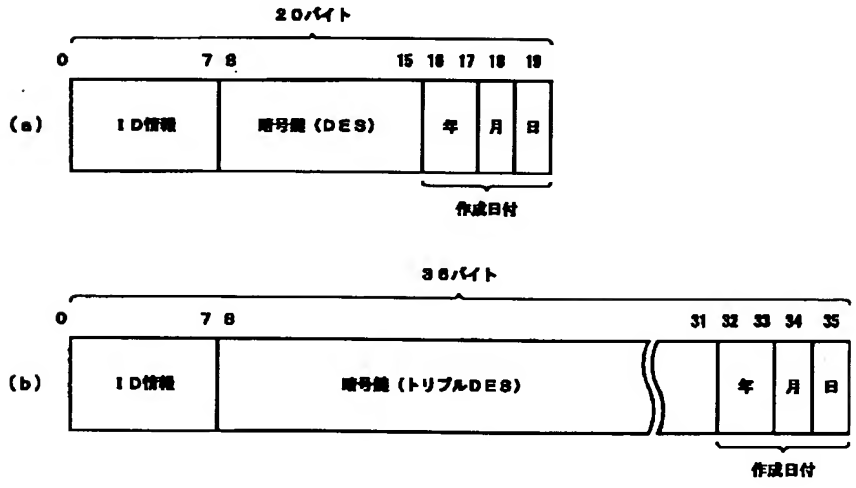
【図2】


(a)
1
1a
(b)
T0
T1
T2
T3
T4
T5
T6
T7
PCA
PMA
R1
UA
RO

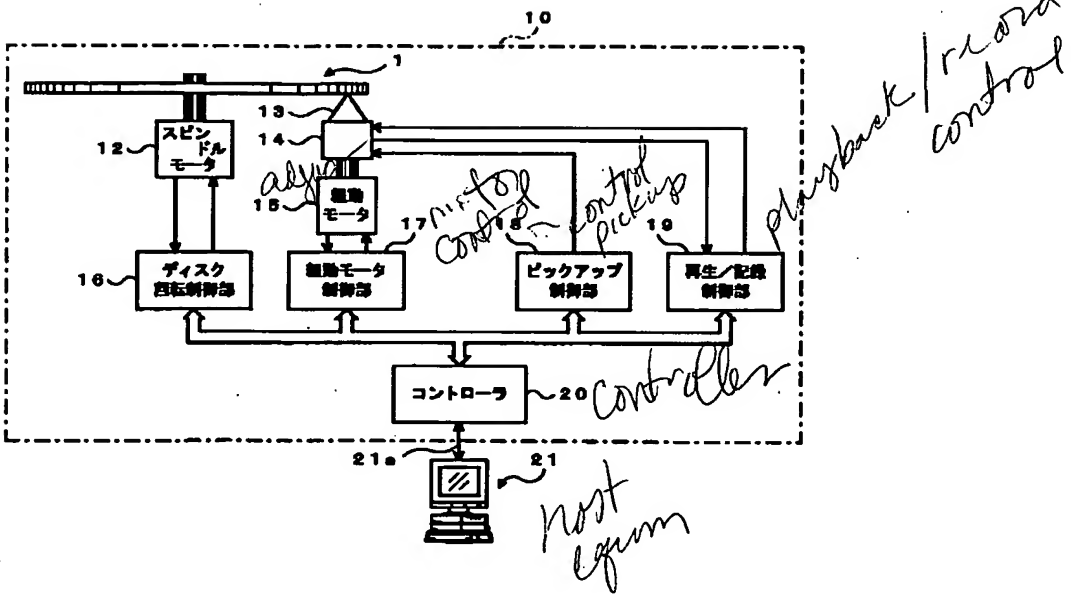
【図3】


1
1a
表
1e
1d
1c
1b
1f
裏

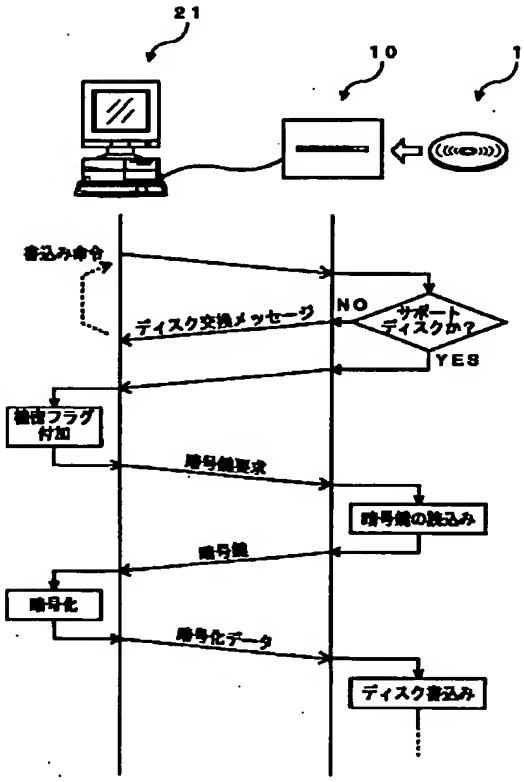
【図5】


20バイト
0
7 8
15 16 17 18 19
(a)
ID情報
暗号鍵 (DES)
年
月
日
作成日付
36バイト
0
7 8
31 32 33 34 35
(b)
ID情報
暗号鍵 (トリプルDES)
年
月
日
作成日付

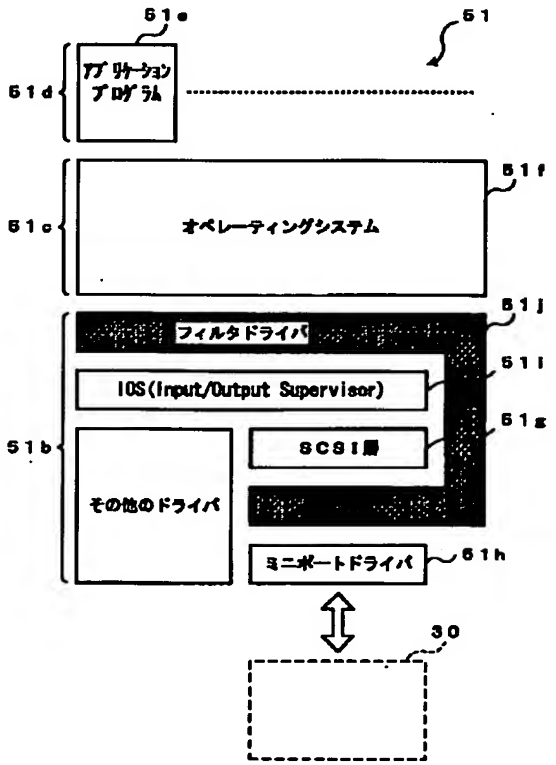
【図6】


10
1
13
12
スピンドルモータ
14
15
16
ディスク回転制御部
17
18
19
ピックアップ制御部
再生/記録制御部
コントローラ
20
21a
21

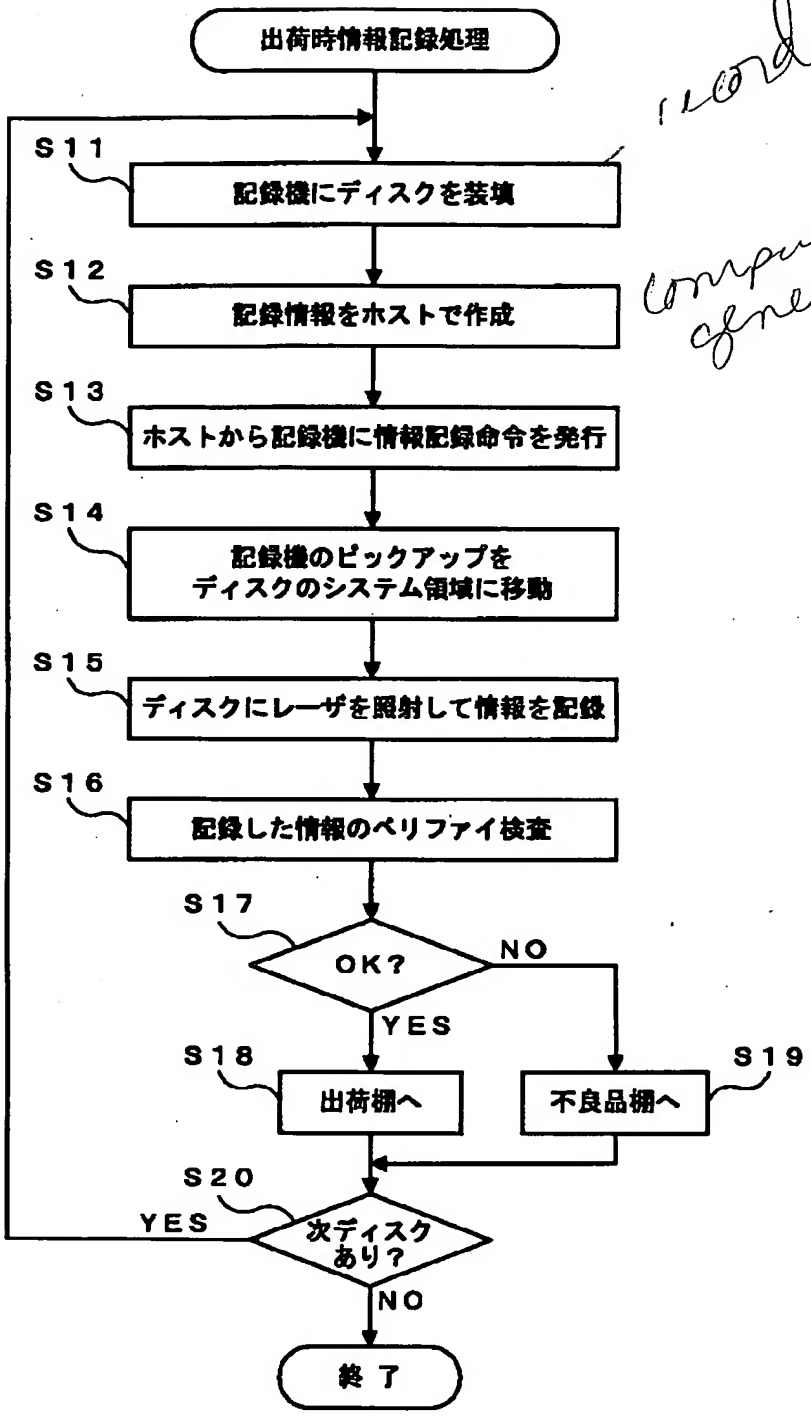
【図9】


21
10
1
書込み命令
ディスク交換メッセージ
NO
サポートディスクか?
YES
暗号フラグ付加
暗号鍵要求
暗号鍵の読込み
暗号鍵
暗号化
暗号化データ
ディスク書込み

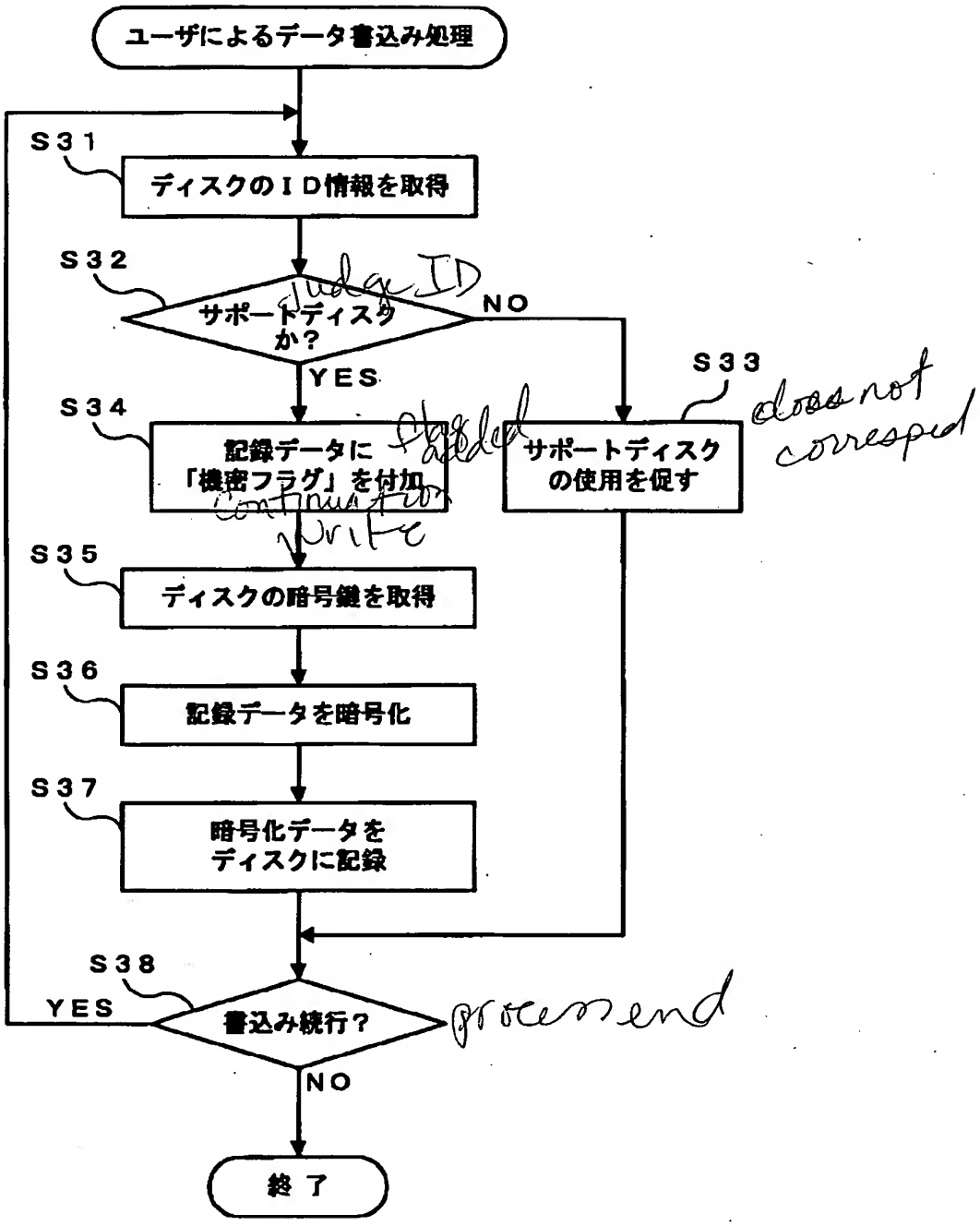
【図11】


51e
51
51d
アプリケーションプログラム
51f
51c
オペレーティングシステム
51j
フィルタドライバ
51i
IOS(Input/Output Supervisor)
51g
51b
SCSI層
その他のドライバ
ミニポートドライバ
51h
30

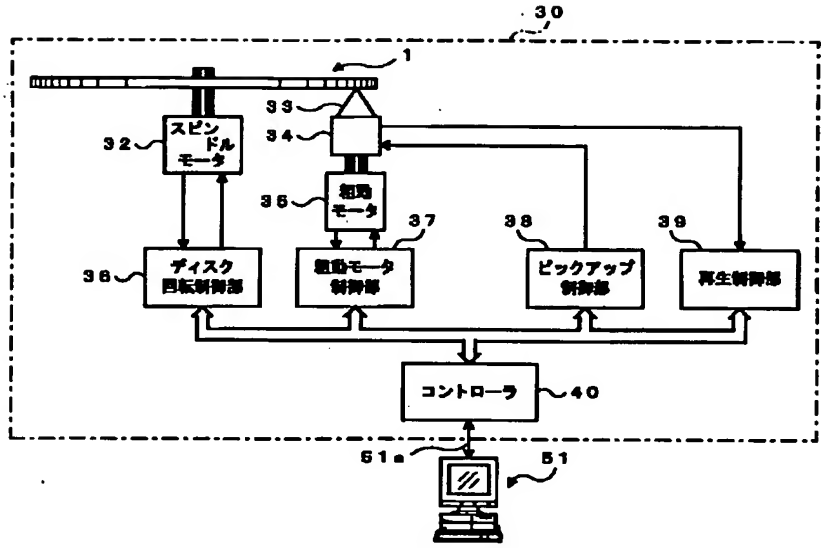
【図7】


出荷時情報記録処理
S11
記録機にディスクを装填
S12
記録情報をホストで作成
S13
ホストから記録機に情報記録命令を発行
S14
記録機のピックアップを
ディスクのシステム領域に移動
S15
ディスクにレーザを照射して情報を記録
S16
記録した情報のベリファイ検査
S17
OK?
NO
YES
S18
出荷棚へ
S19
不良品棚へ
S20
次ディスク
あり?
YES
NO
終了

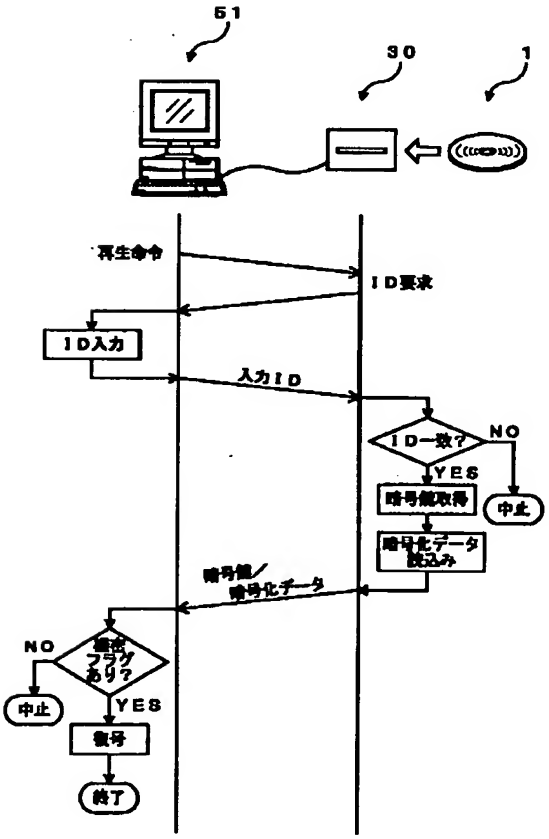
【図8】


ユーザによるデータ書込み処理
S31
ディスクのＩＤ情報を取得
S32
judge ID
サポートディスクか？
NO
YES
S33
does not correspond
S34
flagged
記録データに「機密フラグ」を付加
サポートディスクの使用を促す
continue for write
S35
ディスクの暗号鍵を取得
S36
記録データを暗号化
S37
暗号化データをディスクに記録
S38
YES
書込み続行？
process end
NO
終了

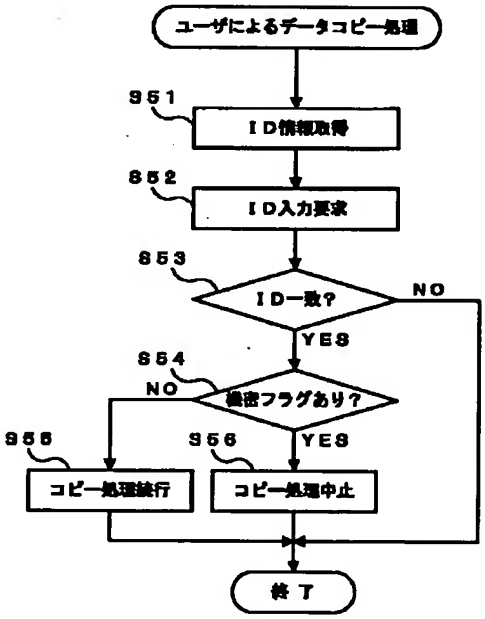
【図10】


30
1
33
34
32
スピンドルモータ
35
粗動モータ
37
38
39
36
ディスク回転制御部
粗動モータ制御部
ピックアップ制御部
再生制御部
コントローラ
40
51a
51

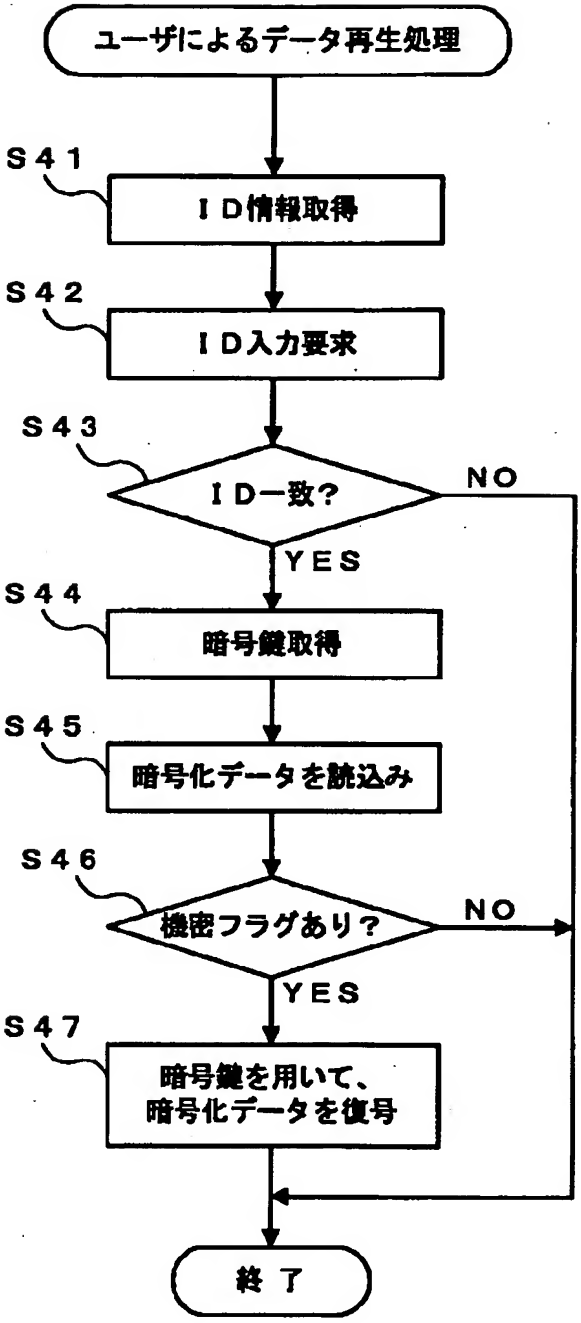
【図13】


51
30
1
再生命令
ID要求
ID入力
入力ID
ID一致?
NO
YES
中止
暗号鍵取得
暗号化データ読込み
暗号鍵/暗号化データ
暗号化フラグあり?
NO
YES
中止
復号
終了

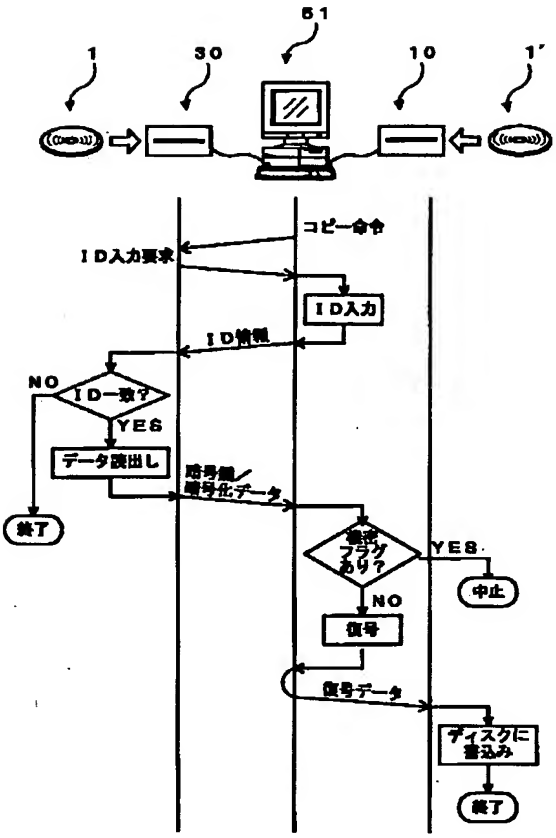
【図14】


ユーザによるデータコピー処理
S51
ID情報取得
S52
ID入力要求
S53
ID一致?
NO
YES
S54
NO
機密フラグあり?
YES
S55
S56
コピー処理続行
コピー処理中止
終了

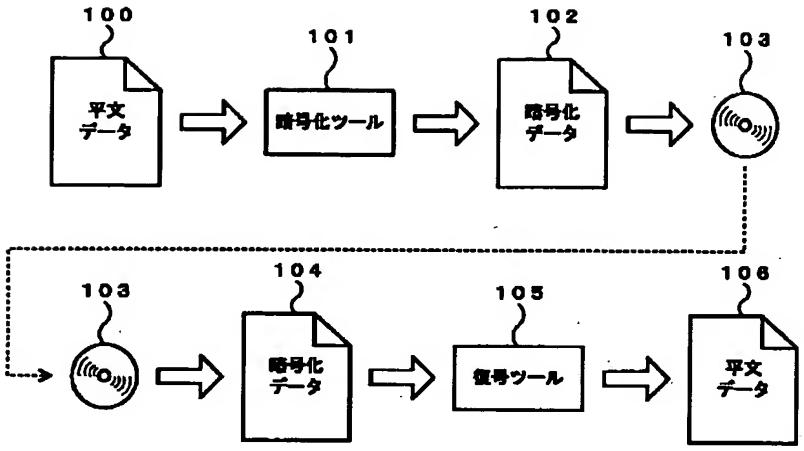
【図12】


ユーザによるデータ再生処理
S41
ＩＤ情報取得
S42
ＩＤ入力要求
S43
ＩＤ一致?
NO
YES
S44
暗号鍵取得
S45
暗号化データを読込み
S46
機密フラグあり?
NO
YES
S47
暗号鍵を用いて、
暗号化データを復号
終了

【図15】


51
1
30
10
1'
コピー命令
ＩＤ入力要求
ＩＤ入力
ＩＤ情報
NO
ＩＤ一致?
YES
データ読出し
暗号鍵
暗号化データ
終了
機密フラグあり?
YES
中止
NO
復号
復号データ
ディスクに書込み
終了

【図16】



フロントページの続き

(72)発明者　清水　洋信
東京都台東区上野6丁目16番20号　太陽誘電株式会社内

Fターム(参考)　5D044 BC05 CC04 DE17 DE60 EF05 FG18 GK12 HL08